

## CLAIMS

We claim:

1. A method comprising:

maintaining an AP database that includes information about managed access point (APs) and friendly APs of a wireless network, including the MAC address of each managed AP;

sending a scan request to one or more managed APs of the wireless network, the scan request including one or more of a request for the receiving managed AP to scan for beacons and probe responses and a request for the receiving managed AP to request the AP's clients to scan for beacons and probe responses;

receiving reports from at least one of the receiving managed APs, a report including information on any beacon or probe response received that was sent by an AP, including the MAC address of the beacon/probe response sending AP; and

for each beacon or probe response on which information is received, analyzing the information received in the report about the AP that sent the beacon or probe response, the analyzing including ascertaining if the MAC address of the AP that sent the beacon or probe response matches a MAC address of an AP in the AP database to ascertain whether or not the AP is a potential rogue AP or a managed or friendly AP.

2. A method as recited in claim 1, wherein the wireless network substantially conforms to the IEEE 802.11 standard for wireless local area networks.

3. A method as recited in claim 1, wherein the maintaining the AP database includes updating the AP database from time to time.

4. A method as recited in claim 1, wherein the analyzing further includes comparing information in the received report related to the beacon or probe response with information stored in the AP database about the configuration of managed APs.

5. A method as recited in claim 4, wherein the analysis further includes determining the approximate location of the potential rogue AP in order to further ascertain whether the potential rogue AP is likely to be a rogue.
6. A method as recited in claim 1, wherein the sending a request includes sending a request to one or more of the wireless stations to scan for beacons and probe responses on the respective serving channels of the respective wireless stations and to report the results of the listening.
7. A method as recited in claim 1, wherein the sending a request includes sending a request for one or more of the wireless stations to temporarily listen for beacons and probe responses on a channel specified in the request and to report the results of the listening.
8. A method as recited in claim 1, wherein the sending a request includes sending a request for one or more managed access points to listen for beacons and probe responses and to report the results of the listening.
9. A method as recited in claim 1, wherein the sending a request includes sending a request for one or more clients of one or more managed access points to listen for beacons and probe responses and to report the results of the listening.
10. A method as recited in claim 1, wherein the analyzing includes comparing configuration information in the beacon or probe response with information stored in the AP database about managed APs.
11. A method as recited in claim 10, wherein the analyzing further includes using timing information determined from the beacon or probe response to further ascertain whether the AP is likely to be a rogue.
12. A method as recited in claim 11, wherein the analyzing further includes using known location information of managed APs together with the timing information to determine the approximate location of the potential rogue AP.

13. A method as recited in claim 10, wherein the analyzing further includes using known location information of managed APs to approximately locate the potential rogue AP, and method further comprising:

locating the potential rogue AP by using the RSSI at the station receiving the beacon or probe response together with a calibrated path loss model of an area of interest that provides path losses at various locations to or from managed stations at known locations.

14. A method as recited in claim 13, wherein the locating includes:

accepting an ideal path loss model applicable to an area of interest;

calibrating the ideal path loss model using measurements received from each respective managed station of a first set of managed wireless stations of the wireless network measuring the received signal strengths at each of the respective managed stations, the managed stations receiving signals as a result of transmissions by respective managed stations of a second set of managed wireless stations of the wireless network, each respective transmission at a known respective transmit power, the locations of each managed station of the first and second set being known or determined, the calibrating being to determine a calibrated path loss model between the receiving and transmitting wireless stations;

receiving measurements from each respective managed station of a third set of managed wireless stations of the wireless network measuring the received signal strength at each of the respective stations resulting from transmission of a beacon or probe response from a potential rogue access point, each station of the third set being at a known or determined location; and

for each of a set of assumed transmit powers for the potential rogue access point, determining the likely location or locations of the potential rogue access point using the received signal strengths at the stations of the third set and the calibrated path loss model.

15. A method as recited in claim 14, wherein the determining of the likely location or locations includes:

determining a set of likelihood components for each of a set of locations, each component corresponding to a respective managed access point whose transmissions are listened for at the particular station, and

determining an overall likelihood for each of the set of locations as the product of the likelihood components.

16. A method as recited in claim 1, wherein further comprising combining the results of the analyzing step with the results of one or more complementary rogue AP detection techniques.

17. A method as recited in claim 16, wherein one of the complementary rogue AP detection techniques includes a client reporting to a managed AP a failed previous authentication attempt with an AP.

18. A method comprising:

receiving a scan request at an AP of a wireless network to scan for beacons and probe responses, the request received from a WLAN manager managing a set of managed APs and client stations of the managed APs, the managing including maintaining an AP database that contains information about managed APs and friendly APs of the wireless network, the information in the AP database including the MAC address of each managed AP;

one or both of listening for beacons and probe responses at the AP receiving the scan request or sending a client request to one or more client stations associated with the AP receiving the scan request to listen for beacons and probe responses;

in the case that a client request was sent, receiving a client report at the AP from at least one of the wireless stations to which the client request was sent, the client report including information on any beacon or probe response received from a potential rogue AP; and

sending a scan report to the WLAN manager including information on any beacon or probe response received from a potential rogue AP by the AP receiving the scan request or in the case that a client request was sent, by any client stations from a report was received, the information including the MAC address of the potential rogue AP.

such that for each beacon or probe response on which information is received at the WLAN manager, analyzing the information received in the report about the potential rogue AP that sent the beacon or probe response, including ascertaining if the MAC address of the potential rogue AP matches a MAC address of an AP in the AP database leads to ascertaining whether or not the potential AP is likely to be a rogue AP.

19. A method as recited in claim 18, wherein the scan request includes a request to scan for beacons and probe responses on the respective serving channel of each respective wireless AP or client station and to report the results of the listening.
20. A method as recited in claim 18, wherein the scan request includes a request for the listening stations AP or client station to temporarily listen for beacons and probe responses on a channel specified in the request and to report the results of the listening.
21. A method as recited in claim 18, wherein the scan request from the WLAN manager and the scan report to the WLAN manager use a protocol that provides for and encapsulates scan request messages and scan report messages in IP packets.
22. A method as recited in claim 21, wherein the request from an AP to a client station, and the report from the client station to an AP uses MAC frames.
23. A method as recited in claim 21, wherein the scan request includes a set of scan parameters that describe how information is to be obtained about beacons and probe responses received by the managed AP or clients thereof.
24. A method as recited in claim 23, wherein the scan parameters include one or more of:
  - whether the requested scan is an active scan or a passive scan or both an active and passive scan, and if an active scan, the one or more channels for the active scan,

the schedule of how often scans are to be performed, and  
whether the performing of the scan is to be by the AP receiving the scan request,  
the managed clients thereof, or both the AP and AP's clients.

25. A method as recited in claim 23, wherein after receiving the task request, the receiving AP sets up tasking according to the scan request, including scheduling any scans to be performed by the receiving AP itself, and also, in the case the tasking includes scanning by one or more clients, scheduling scans to be performed by the clients by sending request frames to the appropriate clients.

26. A carrier medium carrying one or more computer-readable code segments to instruct one or more processors of a processing system to execute a method comprising:

maintaining an AP database that includes information about managed access point (APs) and friendly APs of a wireless network, including the MAC address of each managed AP;

sending a scan request to one or more managed APs of the wireless network, the scan request including one or more of a request for the receiving managed AP to scan for beacons and probe responses and a request for the receiving managed AP to request the AP's clients to scan for beacons and probe responses;

receiving reports from at least one of the receiving managed APs, a report including information on any beacon or probe response received that was sent by an AP, including the MAC address of the beacon/probe response sending the AP; and

for each beacon or probe response on which information is received, analyzing the information received in the report about the AP that sent the beacon or probe response, the analyzing including ascertaining if the MAC address of the AP that sent the beacon or probe response matches a MAC address of an AP in the AP database to ascertain whether or not the AP is a potential rogue AP or a managed or friendly AP.

27. A carrier medium carrying one or more computer-readable code segments to instruct one or more processors of a processing system to execute a method at an AP of a wireless network comprising:

receiving a scan request to scan for beacons and probe responses, the request received from a WLAN manager managing a set of managed APs and client stations of the managed APs, the managing including maintaining an AP database that contains information about managed APs and friendly APs of the wireless network, including the MAC address of each managed AP;

one or both of listening for beacons and probe responses at the AP receiving the scan request or sending a client request to one or more client stations of the AP receiving the scan request to listen for beacons and probe responses;

in the case that a client request was sent, receiving a client report from at least one of the wireless stations to which the client request was sent, the client report including information on any beacon or probe response received from a potential rogue AP; and

sending a scan report to the WLAN manager including information on any beacon or probe response received from a potential rogue AP by the AP receiving the scan request or, in the case that a client request was sent by any client stations from which a report was received, the scan report including the MAC address of any AP whose beacon/probe response was received,

such that for each beacon or probe response on which information is received at the WLAN manager, analyzing the information received in the report about the potential rogue AP that sent the beacon or probe response, including ascertaining if the MAC address of the potential rogue AP matches a MAC address of an AP in the AP database leads to ascertaining whether or not the potential AP is likely to be a rogue AP.

28. An apparatus comprising:

a processing system including a memory and a network interface to couple the apparatus to a network, the network including a set of managed access points (APs) of a wireless network, and

an AP database coupled to the processing system and containing information about the managed access point and friendly APs of the wireless network,

the processing system programmed to:

send a scan request to one or more managed APs of the wireless network, the scan request including one or more of a request for the receiving managed AP to scan for beacons and probe responses and a request for the receiving managed AP to request the AP's clients to scan for beacons and probe responses;

receive reports from at least one of the receiving managed APs, a report including information on any beacon or probe response received that was sent by an AP, including the MAC address of any AP whose beacon/probe response was received; and

for each beacon or probe response on which information is received, analyze the information received in the report about the AP that sent the beacon or probe response, the analyzing including ascertaining if the MAC address of the AP that sent the beacon or probe response matches a MAC address of an AP in the AP database to ascertain whether or not the AP is a potential rogue AP or a managed or friendly AP.

29. An access point (AP) for a wireless network, the access point comprising:

a processing system including a memory;

a network interface to couple the access point to a network;

a wireless transceiver coupled to the processing system to implement the PHY of a wireless station

the processing system including a MAC processor and programmed:

to receive a scan request to scan for beacons and probe responses, the request received via the network interface from a WLAN manager coupled to the network and managing a set of managed APs and client stations of the managed APs, the managing including maintaining an AP database that contains information about managed APs and friendly APs of the wireless network, including the MAC address of each managed AP;

one or both of to listen for beacons and probe responses via the PHY or to send a client request via the PHY to one or more client stations associated with the AP to listen for beacons and probe responses;

in the case that a client request was sent, to receive a client report from at least one of the client stations to which the client request was sent, the client report including information on any beacon or probe response received at the client station from a potential rogue AP; and

to send a scan report to the WLAN manager via the network interface, including information on any beacon or probe response received from a potential rogue AP by the AP receiving the scan request or in the case that a client request was sent, by any client stations from a report was received, the scan report including the MAC address of any AP whose beacon/probe response was received,

such that for each beacon or probe response on which information is received at the WLAN manager, analyzing the information received in the report about the potential rogue AP that sent the beacon or probe response, including ascertaining if the MAC address of the potential rogue AP matches a MAC address of an AP in the AP database leads to ascertaining whether or not the potential AP is likely to be a rogue AP.